UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,420	03/16/2004	Charu C. Aggarwal	YOR920040039US1	2046

7590 09/07/2006

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
LOVEL, KIMBERLY M	

ART UNIT	PAPER NUMBER
2167	

DATE MAILED: 09/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/801,420	AGGARWAL ET AL.	
	Examiner	Art Unit	
	Kimberly Lovel	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/20/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-31 are rejected.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 20 August 2004 was filed after the mailing date of the application on 16 March 2004. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-15 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

MPEP 2106 IV.B.2.(b)

A claim that requires one or more acts to be performed defines a process. However, not all processes are statutory under 35 U.S.C. 101. Schrader, 22 F.3d at 296, 30 USPQ2d at 1460. To be statutory, a claimed computer-related process must either: (A) result in a physical transformation outside the computer for which a practical application is either disclosed in the specification or would have been known to a skilled artisan, or (B) be limited to a practical application.

Claim 1 recites a method for monitoring abnormalities in a data stream, comprising the steps of: receiving a plurality of objects in the data stream; creating one or more clusters from the plurality of objects, wherein at least a portion of the one or more clusters comprise statistical data of the respective cluster; and determining from the statistical data whether one or more abnormalities exist in the data stream in order to quickly determine the reasoning for low similarity values.

The claim is directed towards determining abnormalities. However, the claim fails to produce an output or store a result and therefore fails to produce a tangible result. In order for the subject matter to be considered statutory, it must produce a useful, concrete and tangible result. Claims 2-15 which are dependent on the method of claim 1 fail to overcome the deficiencies of claim 1, and therefore are rejected on the same grounds.

To allow for compact prosecution, the examiner will apply prior art to these claims as best understood, with the assumption that applicant will amend to overcome the stated 101 rejections.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 1-5, 8, 9, 11-20, 23, 24 and 26-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,947,933 to Smolsky (hereafter Smolsky) in view of US PGPub 2004/0098617 to Sekar et al (hereafter Sekar et al).

Referring to claim 1, Smolsky discloses a method for monitoring abnormalities [outliers] in a data stream [stream of data] (see abstract and column 12, lines 24-33 – determining which outliers cause the data to appear non-normal), comprising the steps of:

receiving a plurality of objects [chunks] in the data stream [stream of data] (see column 9, lines 16-17 and Fig 4, item 400) (column 8, lines 44-45) and

creating [building] one or more clusters from the plurality of objects [hierarchical structure 600 of clusters] (see column 13, lines 13-14), wherein at least a portion of the one or more clusters comprise statistical data [Fourier coefficients] of the respective cluster (see column 9, lines 4-14 and column 14, lines 53 – column 15, line 2).

However, Smolsky fails to explicitly disclose the limitation of determining from the statistical data whether one or more abnormalities exist in the data stream. Sekar also discloses a method for monitoring abnormalities in a data stream (see abstract) including the limitation of determining from the statistical data whether one or more abnormalities [anomaly] exist in the data stream [IP packet stream] (see [0032], lines 32-33 and [0041], lines 2-5) in order to quickly determine the reasoning for low similarity values.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the statistical data of Sekar to determine abnormalities in the data of Smolsky. One would have been motivated to do so since if an object has a low similarity value in comparison with many objects, then there is high probability of the occurrence of abnormalities.

Referring to claim 2, Smolsky/Sekar discloses the method of claim 1, wherein the step of creating one or more clusters further comprises:

computing one or more similarity values for a given object relating to one or more existing clusters (Smolsky: see column 10, lines 2-5); and

determining a closest cluster for the object based on the one or more similarity values (Smolsky: see column 15, line 62 – column 16, line 7).

Referring to claim 3, Smolsky/Sekar discloses the method of claim 2, further comprising the steps of:

determining whether to add the object to the closest cluster (Smolsky: see column 15, line 62 – column 16, line 7);

adding the object to the closest cluster when determined and updating the statistical data of the closest cluster (Smolsky: see column 15, line 62 – column 16, line 7); and

creating a new cluster comprising the object when the object is not added to the closest cluster (Smolsky: see column 13, lines 31-35), and generating statistical data of the new cluster (Smolsky: see column 9, lines 4-14 and column 14, lines 53 – column 15, line 2).

Referring to claim 4, Smolsky/Sekar discloses the method of claim 3, wherein the step of determining whether to add the object to the closest cluster further comprises the step of determining if the similarity value is greater than a user-defined threshold (Smolsky: see column 16, lines 35-38).

Referring to claim 5, Smolsky/Sekar discloses the method of claim 1, wherein the step of determining from the statistical data whether one or more abnormalities exist further comprises the steps of:

determining which clusters present at a first time [t0] were not present at a second time [t2], wherein the second time is before the first time (Sekar: see Fig 2 and column 6, lines 29-38);

determining which of the clusters, present at the first time and not present at the second time, contain fewer than a user-defined number of objects (Sekar: see column 12, lines 31-33); and

reporting clusters with fewer than the user-defined number of objects as abnormalities (Sekar: see column 12, lines 31-33).

Referring to claim 8, Smolsky/Sekar discloses the method of claim 1, wherein the statistical data of each cluster comprises one or more statistical counts of each categorical attribute (Sekar: see [0088], lines 1-7).

Referring to claim 9, Smolsky/Sekar discloses the method of claim 1, wherein the statistical data of each cluster comprises a number of objects in each cluster (Sekar: see [0088], lines 1-7).

Referring to claim 11, Smolsky/Sekar discloses the method of claim 1, wherein the step of creating one or more clusters further comprises the step of applying one or more weights to one or more attributes (Smolsky: see column 16, lines 1-7).

Referring to claim 12, Smolsky/Sekar discloses the method of claim 1, wherein abnormalities comprise intrusions in a network (Sekar: see abstract).

Referring to claim 13, Smolsky/Sekar discloses the method of claim 12, wherein the step of receiving a plurality of objects further comprises the step of collecting source IP (Internet Protocol) address data [source address], destination IP address data [destination address] (Smolsky: see column 5, line 34 and line 45 – collecting address) and signature data [trace of state machine] (Sekar: see [0021]).

Referring to claim 14, Smolsky/Sekar discloses the method of claim 12, wherein the step of creating one or more clusters further comprises the step of clustering source IP address data, destination IP address data and signature data (Smolsky: see column 13, lines 13-14).

Referring to claim 15, Smolsky/Sekar discloses the method of claim 12, wherein the step of determining from the statistical data whether one or more abnormalities exist

further comprises the step of detecting one or more intrusions from statistical data of source IP address data, destination IP address data and signature data (Sekar: see [0032]).

Referring to claim 16, Smolsky discloses an apparatus for monitoring abnormalities [outliers] in a data stream [stream of data] (see abstract and column 12, lines 24-33 – determining which outliers cause the data to appear non-normal), comprising:

a memory (see column 8, lines 21-27); and

at least one processor coupled to a memory (Enterprise SDE Server 104) and operative to:

(i) receive a plurality of objects [chunks] in the data stream [stream of data] (see column 9, lines 16-17 and Fig 4, item 400) (column 8, lines 44-45) and

(ii) create [building] one or more clusters from the plurality of objects [hierarchical structure 600 of clusters] (see column 13, lines 13-14), wherein at least a portion of the one or more clusters comprise statistical data [Fourier coefficients] of the respective cluster (see column 9, lines 4-14 and column 14, lines 53 – column 15, line 2).

However, Smolsky fails to explicitly disclose the limitation of determining from the statistical data whether one or more abnormalities exist in the data stream. Sekar also discloses a method for monitoring abnormalities in a data stream (see abstract) including the limitation of (iii) determine from the statistical data whether one or more abnormalities [anomaly] exist in the data stream [IP packet stream] (see [0032], lines

32-33 and [0041], lines 2-5) in order to quickly determine the reasoning for low similarity values.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the statistical data of Sekar to determine abnormalities in the data of Smolsky. One would have been motivated to do so since if an object has a low similarity value in comparison with many objects, then there is high probability of the occurrence of abnormalities.

Referring to claim 17, Smolsky/Sekar discloses the apparatus of claim 16, wherein the operation of creating one or more clusters further comprises:

computing one or more similarity values for a given object relating to one or more existing clusters (Smolsky: see column 10, lines 2-5); and

determining a closest cluster for the object based on the one or more similarity values (Smolsky: see column 15, line 62 – column 16, line 7).

Referring to claim 18, Smolsky/Sekar discloses the apparatus of claim 17, further comprising:

determining whether to add the object to the closest cluster (Smolsky: see column 15, line 62 – column 16, line 7);

adding the object to the closest cluster when determined and updating the statistical data of the closest cluster (Smolsky: see column 15, line 62 – column 16, line 7); and

creating a new cluster comprising the object when the object is not added to the closest cluster (Smolsky: see column 13, lines 31-35), and generating statistical data of

the new cluster (Smolsky: see column 9, lines 4-14 and column 14, lines 53 – column 15, line 2).

Referring to claim 19, Smolsky/Sekar discloses the apparatus of claim 18, wherein the step of determining whether to add the object to the closest cluster further comprises the step of determining if the similarity value is greater than a user-defined threshold (Smolsky: see column 16, lines 35-38).

Referring to claim 20, Smolsky/Sekar discloses the apparatus of claim 17, wherein the operation of determining from the statistical data whether one or more abnormalities exist further comprises:

determining which clusters present at a first time [t0] were not present at a second time [t2], wherein the second time is before the first time (Sekar: see Fig 2 and column 6, lines 29-38);

determining which of the clusters, present at the first time and not present at the second time, contain fewer than a user-defined number of objects (Sekar: see column 12, lines 31-33); and

reporting clusters with fewer than the user-defined number of objects as abnormalities (Sekar: see column 12, lines 31-33).

Referring to claim 23, Smolsky/Sekar discloses the apparatus of claim 16, wherein the statistical data of each cluster comprises one or more statistical counts of each categorical attribute (Sekar: see [0088], lines 1-7).

Referring to claim 24, Smolsky/Sekar discloses the apparatus of claim 16, wherein the statistical data of each cluster comprises a number of objects in each cluster (Sekar: see [0088], lines 1-7).

Referring to claim 26, Smolsky/Sekar discloses the apparatus of claim 16, wherein the step of creating one or more clusters further comprises the step of applying one or more weights to one or more attributes (Smolsky: see column 16, lines 1-7).

Referring to claim 27, Smolsky/Sekar discloses the apparatus of claim 16, wherein abnormalities comprise intrusions in a network (Sekar: see abstract).

Referring to claim 28, Smolsky/Sekar discloses the apparatus of claim 27, wherein the step of receiving a plurality of objects further comprises the step of collecting source IP (Internet Protocol) address data [source address], destination IP address data [destination address] (Smolsky: see column 5, line 34 and line 45 – collecting address) and signature data [trace of state machine] (Sekar: see [0021]).

Referring to claim 29, Smolsky/Sekar discloses the apparatus of claim 27, wherein the step of creating one or more clusters further comprises the step of clustering source IP address data, destination IP address data and signature data (Smolsky: see column 13, lines 13-14).

Referring to claim 30, Smolsky/Sekar discloses the apparatus of claim 27, wherein the step of determining from the statistical data whether one or more abnormalities exist further comprises the step of detecting one or more intrusions from statistical data of source IP address data, destination IP address data and signature data (Sekar: see [0032]).

Referring to claim 31, Smolsky discloses an article of manufacture for monitoring abnormalities [outliers] in a data stream [stream of data] (see abstract and column 12, lines 24-33 – determining which outliers cause the data to appear non-normal), comprising a machine readable medium containing one or more programs which when executed implement the steps of:

receiving a plurality of objects [chunks] in the data stream [stream of data] (see column 9, lines 16-17 and Fig 4, item 400) (column 8, lines 44-45) and

creating [building] one or more clusters from the plurality of objects [hierarchical structure 600 of clusters] (see column 13, lines 13-14), wherein at least a portion of the one or more clusters comprise statistical data [Fourier coefficients] of the respective cluster (see column 9, lines 4-14 and column 14, lines 53 – column 15, line 2).

However, Smolsky fails to explicitly disclose the limitation of determining from the statistical data whether one or more abnormalities exist in the data stream. Sekar also discloses a method for monitoring abnormalities in a data stream (see abstract) including the limitation of determining from the statistical data whether one or more abnormalities [anomaly] exist in the data stream [IP packet stream] (see [0032], lines 32-33 and [0041], lines 2-5) in order to quickly determine the reasoning for low similarity values.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the statistical data of Sekar to determine abnormalities in the data of Smolsky. One would have been motivated to do so since if an object has a low

similarity value in comparison with many objects, then there is high probability of the occurrence of abnormalities.

7. Claims 6, 7, 10, 21, 22 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6,947,933 to Smolsky in view of US PGPub 2004/0098617 to Sekar et al as applied respectively to claims 1 and 16 above, and further in view of US Patent No 6,625,585 to MacCuish et al (hereafter MacCuish et al).

Referring to claim 6, Smolsky et al disclose statistical data. However, Smolsky et al fail to explicitly disclose the further limitation wherein the statistical data of each cluster is stored using an incremental updating process. MacCuish et al disclose clustering data (see abstract) including the further limitation wherein the statistical data of each cluster is stored using an incremental updating process (see column 30, lines 42-50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the incremental updating process of MacCuish et al as the type of statistical data utilized by Smolsky et al. One would have been motivated to do so since the data being clustered is being transmitted in a stream which means that new data is constantly being clustered.

Referring to claim 7, Smolsky et al disclose statistical data. However, Smolsky et al fail to explicitly disclose the further limitation wherein the statistical data of each cluster comprises one or more statistical counts of each pairwise attribute. MacCuish et al disclose clustering data (see abstract) including the further limitation wherein the

statistical data of each cluster comprises one or more statistical counts of each pairwise attribute (see column 14, lines 44-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize pairwise attributes of MacCuish et al as the type of statistical data utilized by Smolsky et al. One would have been motivated to do so in order to calculate the similarity of the clusters.

Referring to claim 10, Smolsky et al disclose statistical data. However, Smolsky et al fail to explicitly disclose the further limitation wherein the statistical data is stored periodically at intervals chosen based on a pyramidal distribution. MacCuish et al disclose clustering data (see abstract) including the further limitation wherein the statistical data is stored periodically at intervals chosen based on a pyramidal distribution (see column 14, lines 27-29).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the feature of periodically storing the statistics of MacCuish et al as the type of statistical data utilized by Smolsky et al. One would have been motivated to do so since the data being clustered is being transmitted in a stream which means that new data is constantly being clustered.

Referring to claim 21, Smolsky et al disclose statistical data. However, Smolsky et al fail to explicitly disclose the further limitation wherein the statistical data of each cluster is stored using an incremental updating process. MacCuish et al disclose clustering data (see abstract) including the further limitation wherein the statistical data

of each cluster is stored using an incremental updating process (see column 30, lines 42-50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the incremental updating process of MacCuish et al as the type of statistical data utilized by Smolsky et al. One would have been motivated to do so since the data being clustered is being transmitted in a stream which means that new data is constantly being clustered.

Referring to claim 22, Smolsky et al disclose statistical data. However, Smolsky et al fail to explicitly disclose the further limitation wherein the statistical data of each cluster comprises one or more statistical counts of each pairwise attribute. MacCuish et al disclose clustering data (see abstract) including the further limitation wherein the statistical data of each cluster comprises one or more statistical counts of each pairwise attribute (see column 14, lines 44-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize pairwise attributes of MacCuish et al as the type of statistical data utilized by Smolsky et al. One would have been motivated to do so in order to calculate the similarity of the clusters.

Referring to claim 25, Smolsky et al disclose statistical data. However, Smolsky et al fail to explicitly disclose the further limitation wherein the statistical data is stored periodically at intervals chosen based on a pyramidal distribution. MacCuish et al disclose clustering data (see abstract) including the further limitation wherein the

statistical data is stored periodically at intervals chosen based on a pyramidal distribution (see column 14, lines 27-29).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the feature of periodically storing the statistics of MacCuish et al as the type of statistical data utilized by Smolsky et al. One would have been motivated to do so since the data being clustered is being transmitted in a stream which means that new data is constantly being clustered.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kimberly Lovel whose telephone number is (571) 272-2750. The examiner can normally be reached on 8:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Cottingham can be reached on (571) 272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kimberly Lovel
Examiner
Art Unit 2167

1 Sept 2006
kml

JOHN COTTINGHAM
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1 September 2006